A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets

HANAN HINDY, Division of Cyber Security, Abertay University, Scotland
DAVID BROSSET, Naval Academy Research Institute, France
ETHAN BAYNE, Division of Cyber Security, Abertay University, Scotland
AMAR SEEAM, Department of Computer Science, Middlesex University, Mauritius
CHRISTOS TACHTATZIS, EEE Department, University of Strathclyde, Scotland
ROBERT ATKINSON, EEE Department, University of Strathclyde, Scotland
XAVIER BELLEKENS, Division of Cyber Security, Abertay University, Scotland

With the world moving towards being increasingly dependent on computers and automation, one of the main challenges in the current decade has been to build secure applications, systems and networks. Alongside these challenges, the number of threats is rising exponentially due to the attack surface increasing through numerous interfaces offered for each service. To alleviate the impact of these threats, researchers have proposed numerous solutions; however, current tools often fail to adapt to ever-changing architectures, associated threats and 0-days. This manuscript aims to provide researchers with a taxonomy and survey of current dataset composition and current Intrusion Detection Systems (IDS) capabilities and assets. These taxonomies and surveys aim to improve both the efficiency of IDS and the creation of datasets to build the next generation IDS as well as to reflect networks threats more accurately in future datasets. To this end, this manuscript also provides a taxonomy and survey or network threats and associated tools. The manuscript highlights that current IDS only cover 25% of our threat taxonomy, while current datasets demonstrate clear lack of real-network threats and attack representation, but rather include a large number of deprecated threats, hence limiting the accuracy of current machine learning IDS. Moreover, the taxonomies are open-sourced to allow public contributions through a Github repository.

ACM Reference Format:
Hanan Hindy, David Brosset, Ethan Bayne, Amar Seeam, Christos Tachtatzis, Robert Atkinson, and Xavier Bellekens. 2018. A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets. 1, 1 (June 2018), 35 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The world is becoming more dependent on connected actuators and sensors, regulating the life of millions of people. Furthermore, sensor data is expected to increase by around 13%, reaching 35% of overall data communication by 2020, reaching a peak of 50 billion connected devices and an increased Internet traffic reaching 30 GB on average per capita compared to around 10 GB in

Authors' addresses: Hanan Hindy, Division of Cyber Security, Abertay University, Bell Street, Dundee, DD1 1HG, Scotland, 1704847@abertay.ac.uk; David Brosset, Naval Academy Research Institute, Lanveoc, France; Ethan Bayne, Division of Cyber Security, Abertay University, Bell Street, Dundee, DD1 1HG, Scotland; Amar Seeam, Department of Computer Science, Middlesex University, Mauritius; Christos Tachtatzis, EEE Department, University of Strathclyde, Glasgow, Scotland; Robert Atkinson, EEE Department, University of Strathclyde, Glasgow, Scotland; Xavier Bellekens, Division of Cyber Security, Abertay University, Bell Street, Dundee, DD1 1HG, Scotland, x.bellekens@abertay.ac.uk.

XXXX-XXXX/2018/6-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

2016 [17]. While each of these devices in IoT system exchange collected data, associated services often provide numerous interfaces to interact with the collected data, often increasing the attack surface, highlighting the importance of network security. Therefore, it is crucial to build robust tools to defend networks against security threats. Current detection tools are often based on outdated datasets which, do not reflect the reality of network attacks, rendering the Intrusion Detection Systems (IDS) ineffective against new threats and 0-days. To the best knowledge of the authors, there is currently no survey and taxonomy manuscript analysing available datasets, nor providing a taxonomy of the current network threats and the tools associated with them. The contributions of this paper are threefold:

- An Intrusion detection systems survey and taxonomy is presented, including:
  - An IDS Design Taxonomy
  - IDS Evaluation Metrics
  - A survey of IDS Implementations
- Evaluation of available datasets
- A Threat taxonomy is presented, categorized by:
  - The Threat Sources
  - The Open Systems Interconnection (OSI) Layer
  - Active or Passive modes
  - As well as an example of recent attacks

The rest of the paper is organized as follows; Section 2 depicts the main differences between intrusion detection systems and their main evaluation metrics. In section 3, IDS of the past decade are reviewed and their individual contributions are assessed. Moreover, available datasets are discussed highlighting their drawbacks and limitations. Section 4 provides a threat taxonomy.

2 INTRUSION DETECTION SYSTEMS

IDS are defined as systems built to monitor and analyse network communication, as a result of monitoring, and hence detect anomalies and intrusions.

Current IDS taxonomies focus on a single aspect of the IDS, such as the machine learning algorithms that researchers can potentially use [32] [38], the characteristics of intrusion detection systems [20] [6], or the features that should be used by researchers to design an IDS [91]. While these provide valuable information, these surveys do not provide an global overview dedicated to the design of next-generation IDS, but rather focus on a narrow field. In this section, a broad taxonomy dedicated to the design of intrusion detection system is presented including the different features an IDS can be composed of.

Figure 1 provides a taxonomy of intrusion detections systems. Figure 1 (Branch 1) includes the general attributes characterizing IDS such as their role in the network, the information provided by the intrusion detection system, the system requirements, and their usage. Branch 2 describes the attributes related to the types of decisions, infrastructure in place, as well as their computational location. Branch 3 includes the evaluation metrics. Branch 4 provides a descriptive analysis of their location on the network. Branch 4 also includes an analysis of the triggers. Branch 5 places intrusion detection systems in the context of Mobile Ad hoc Networks (MANETS), and finally, Branch 6 highlights the shortcomings of IDS in the context of Wireless Sensor Networks (WSN) [13]. The different branches are subsequently described in Sections 2.1 through 2.4.

2.1 IDS Design Taxonomy

As mentioned, machine learning based IDS focuses on detecting misbehaviour in networks. When an intrusion is detected the IDS is expected to log the information related to the intrusion (1.1.1).

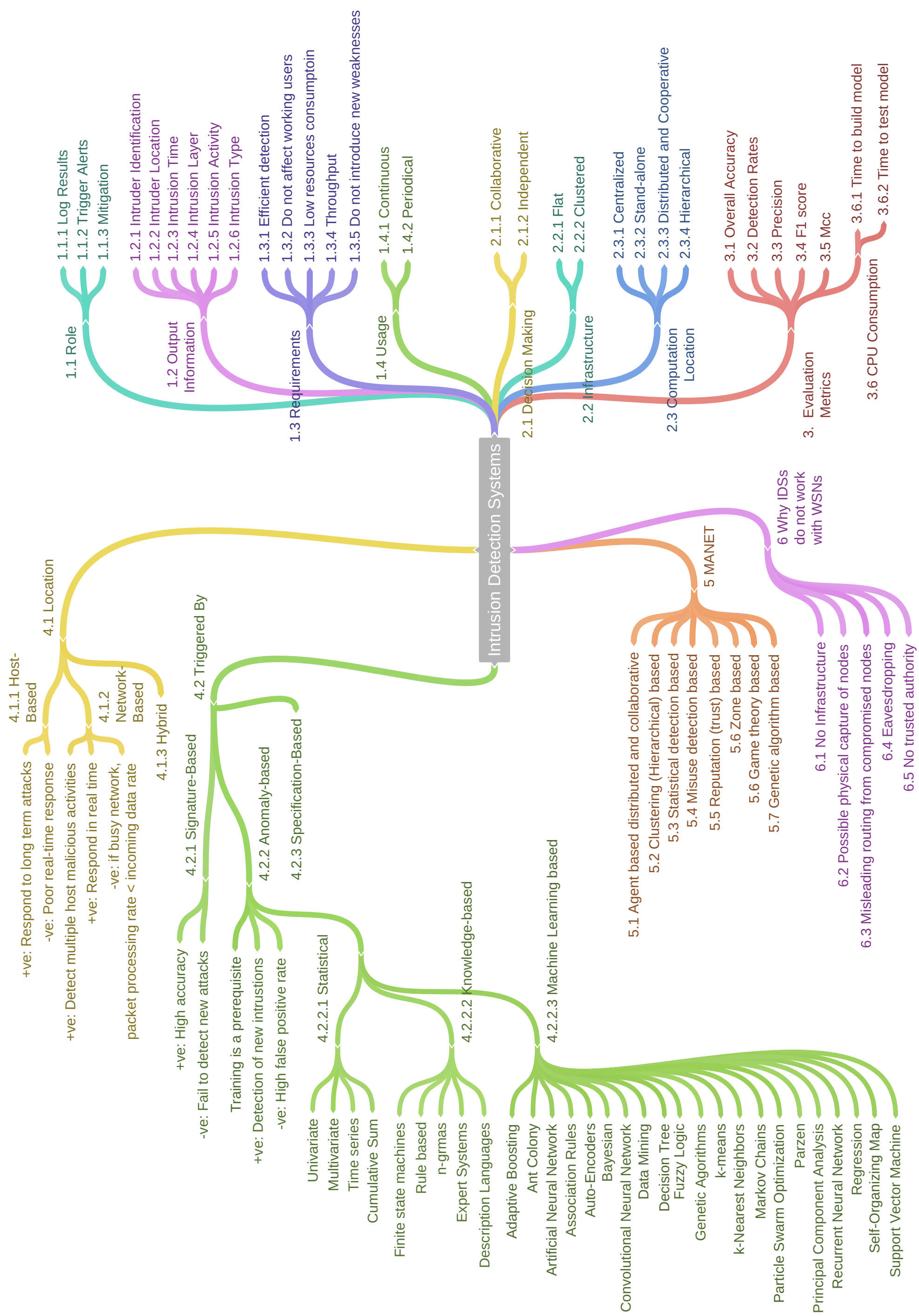


Fig. 1. Intrusion Detection Systems

These logs can then be used by network forensic investigators to further analyse the breach or for the learning process of the IDS itself. IDS are also expected to trigger alerts (1.1.2). The alert should provide information on the threat detected, and the affected system. By raising an alert, authorized users can take corrective action and mitigate the threat. Intrusion Detection System should also include a mitigation feature, giving the ability of the system to take corrective actions (1.1.3) [13].

In order to build an efficient intrusion detection system, the output information provided by the IDS to the end user is critical for analysis. The information recorded should contain intruder identification information (1.2.1) and location (1.2.2) for each event. IP addresses and user credentials are used to identify the intruder. The system design should be modular to adapt to the environment, i.e. [66] propose to use biometric data to identify intruders. Additionally, log information can contain metadata related to the intrusion, such as timestamp (1.2.3), intrusion layer (i.e. OSI) (1.2.4), intrusion activity (1.2.5) whether the attack is active or passive and finally, the type of intrusion(1.2.6) [13].

In order for an IDS to be considered effective, the detection rate (1.3.1) and low false positive rate are key aspects to consider. These can be evaluated using different metrics discussed in section 2.3. Other important factors include the transparency and safety of the overall system (1.3.2). The overall performance of the system has to be taken into account, these include memory requirements, power consumption (1.3.3) and throughput (1.3.4). Lastly, the IDS should not introduce abnormal behavior (1.3.5), hence a testing procedure should be set in place before deployment. The procedure can include fuzzing to detect anomalies and bugs in the IDS. Such anomalies could be exploited by an attacker to render the IDS useless or initiate a denial of service attack [13].

2.2 Distributed IDS

IDS can be distributed over multiple nodes in the network. Intrusion decisions in this case, can be made in a collaborative or swarm like (2.1.1) fashion, or independent (2.1.2) manner. In a collaborative manner, multiple nodes share a single decision. This collaboration can use statistical techniques such as voting and game theory, while in an independent mode, all decisions are made by individual nodes on the network.

Moreover, in this distributed manner, when all nodes are working with the same capacity, it is considered a flat (2.2.1) infrastructure, unlike a clustered infrastructure (2.2.2) where the nodes belong to clusters with different capabilities, each contributing to the decisions in a different manner. The computation location is another aspect of distributed IDS. The centralized computation location (2.3.1) works on data collected from the whole network. Unlike the centralized, the stand-alone computation location (2.3.2) works on local data, disregarding decisions from other nodes. A combination of both centralized and stand-alone, can also be achieved through cooperative computation, such that each node can detect an intrusion on its own but also contributes to the overall decision. Finally, IDS can also operate in hierarchal computation (2.3.4), where a cluster send all intrusion detection to root node, where a decision is taken [13].

2.3 IDS Accuracy

A high detection rate is essential in a machine learning based IDS alongside the evaluation metrics aforementioned. The main aspects to consider when measuring the accuracy are

- True Positive (TP): Number of intrusions correctly detected
- True Negative (TN): Number of non-intrusions correctly detected
- False Positive (FP): Number of non-intrusions incorrectly detected
- False Negative (FN): Number of intrusions incorrectly detected

Hodo *et al.* [38], Buse *et al.* [9] and Aminanto *et al.* [7] discuss the main metrics to consider in their respective work. These include the overall accuracy, decision rates, precision, recall, F1 and Mcc.

$$OverallAccuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

Equation 1 provides the user with the probability that an item is correctly classified by the algorithm.

Detection Rates :

$$\begin{aligned} Sensitivity\ (aka\ Recall) &= \frac{TP}{TP + FN} \\ Specificity &= \frac{TN}{TN + FP} \\ Fallout &= \frac{FP}{TN + FP} \\ Miss\ Rate &= \frac{FN}{TP + FN} \end{aligned} \tag{2}$$

Equation 2 calculates the TP, TN, FP and FN detection rates respectively.

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

Equation 3 provides the percentage of positively classified incidents that are truly positive.

$$F1 = \frac{2TP}{2TP + FP + FN} \tag{4}$$

Equation 4 represents the harmonic mean of precision and recall.

$$Mcc = \frac{(TPxTN) - (FPxFN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \tag{5}$$

Equation 5 provides Matthews correlation coefficient. It can only be used in binary IDS in which incidents are classified as either attack or normal.

Additionally, the CPU consumption, the throughput and the power consumption are important metrics for the evaluation of intrusion detection systems running on different hardware on specific settings such as high-speed networks, or on hardware with limited resources.

2.4 IDS Internals

The location of IDS on the network can tremendously impact the threat detection, hence the overall accuracy of the system. As shown in Figure 1 (4.1), IDS can be located on a host computer, or inline and respond in real time to threats (4.1.2). Note that the detection rate of an inline IDS often degrades when used on a busy network. A hybrid system (4.1.3) being distributed both on the hosts and through the network can also be implemented, using hosts as sensors for swarm intelligence.

The detection method is an important aspect of all intrusion detection system (4.2). Signature-based (4.2.1) IDS are based on prior threat detection and the creation of accurate signatures. The main advantage of this method is the high accuracy for known attacks. The IDS is , however, unable to detect 0-days and polymorphic threats [12]. Signature-based is also known as 'Misuse Detection'. Anomaly-based (4.2.2) depends on identifying patterns and comparing them to normal traffic patterns. This method requires training the system prior to deploying it. The accuracy of such a system against 0-days and polymorphic threats is better when compared against signature-based IDS. However, the false positive rate is often high.

Anomaly-based IDS are based on identifying patterns defining normal and abnormal traffic. These IDS can be classified into subcategories based on the training method used. These categories are identified respectively as statistical, knowledge-based and machine learning based. Statistical (4.2.2.1) includes univariate, multivariate and time series. Knowledge-based (4.2.2.2) uses finite state machines and rules like case-based, n-based, expert systems and descriptor languages. Finally, machine learning includes artificial neural networks, clustering, genetic algorithms, deep learning, . . . Specification-based (4.2.3) combines the strength of both signature and anomaly based to form a hybrid model.

2.5 Industrial IDS

Industrial Intrusion Detection Systems face different challenges, than traditional IDS. The automation of processes included in industrial network architectures often make use of specialized hardware for specific industries such as petrochemical, aerospace, etc. These hardwares use specific communication protocols such as ModBus, Profibus . . .

Table 1 summarizes how the industrial settings differ from traditional ones. Including the dependency on embedded systems, hardware - such as PLC, Data Logger, etc - are an important aspect of the network. Unlike traditional networks, PLCs are unable to run an integrated IDS due to limited processing power. Moreover, the network architecture is fixed and rarely changes, as industrial processes often cover a limited range of functions. These systems can be used for decades without updates. However, industrial processes have a predictable element, which should be taken into account when designing the IDS [106].

Table 1. Industrial Processes VS Traditional Processes

	Industrial Processes	Traditional Processes
Hardware Involvement	Yes	No
Network Topology	Fixed	Dynamic
Functionality	Fixed and Small range	Wide range
Protocols	Simple	Complex
Resources	Limited	Highly accessible
Performance and Availability	Requires real-time	Not dominant requirement
Behaviour	Predictable	Unpredictable

2.6 Feature Selection

"Feature Learning" [7] or "Feature Engineering" [28] plays an important role in building any IDS in a way that chosen features highly affect the accuracy. Different features representations can be used to address different areas of threat detection. Some of them are considered naive when they contain basic information about the software or network. Others are considered rich when they represent deeper details [28].

Obtaining features can be done using one of the following processes or a combination of them.

- Construction
- Extraction
- Selection

Feature construction creates new features by mining existing ones by finding missing relations within features. While extraction works on raw data and/or features and apply mapping functions to extract new ones. Selection works on getting a significant subset of features. This helps reduce the feature space and reduce the computational power.

Feature selection can be done through three approaches, as shown in Table 2, filter, wrapper and embedded.

Table 2. Feature Selection Approaches

Approach	Description	Advantages	Disadvantages
Filter [33]	Selects the most meaningful features regardless the model	Low Execution Time and over-fitting	May choose redundant variables
Wrapper [65]	Combine related variables to have subsets	Consider interactions	Over-fitting risk and High execution time
Embedded [35]	Investigate interaction in a deeper manner than Wrapper	Result in an optimal subset of variables	–

In the following section a survey of recent IDS is presented.

3 IDS AND DATASETS SURVEY

In the past decade numerous IDS were developed and evaluated against a range of published available datasets. In this Section, these datasets are summarized, and their limitations highlighted. Furthermore, recent IDS are analysed discussing algorithms used and the datasets the IDS were evaluated against. Moreover, the trends in the algorithms used by research over the past decade are discussed, highlighting a clear shift in the use of specific algorithms.

3.1 IDS and Associated Datasets

Researchers depended on benchmark datasets to evaluate their results. However, the datasets currently available lack real-life properties. This is the reason that made most of the anomaly intrusion detection systems not applicable for production environments [92], furthermore, they unable of adapting to the constant changes in networks (i.e. new nodes, changing traffic loads, changing topology, etc ...).

Viegas *et al.* [92] mentioned that for a dataset to be considered, it has to cover the following properties: (a) Real network traffic (similar to production ones), (b) Valid, such that it has complete scenarios. (c) Labeled, specifying the class of each record as normal or attack, (d) Variant, (e) Correct, (f) Can be updated easily, (g) Reproducible in order to give researchers the space to compare across different datasets, and finally (h) Sharable, hence it should not contain any confidential data. Additionally, Iman et al [75] mentions that (i) having variant protocols is an important aspect of IDS dataset, as well as (j) having an appropriate documentation for the feature and dataset collection environment.

A benchmark for dataset is presented in [75]. The benchmark include DARPA [49], KDD'99 [36], DEFCON [30], CAIDA [26], LBNL [50], CDX [73], Kyoto [81], Twente [82], UMASS [67], ISCX2012 [27] and ADFA [18]. While the evaluation includes the attacks in each dataset and the features are compared, the authors fail to provide a detailed analysis of the broader impact of their benchmark.

In this manuscript, a survey of machine learning IDS is provided, analyzing the associated datasets and their short-comings.

Table 3.1 introduces the most pre-eminent (i.e. most cited) IDS research from the past decade. Each IDS is mentioned with a list of the algorithms used and the datasets the IDS was evaluated against. Moreover, the attacks detected are also listed.

The algorithmic trends are then discussed alongside the attacks included in the datasets used.

Table 3. A Decade of Intrusion Detection Systems (2008 - 2018)

Year	Authors	Paper Title	Dataset	Used Algorithms	Detected Attacks	Ref
2008	Cheng Xiang *et al.*	Design of Multiple-Level Hybrid Classifier for Intrusion Detection System using Bayesian Clustering and Decision Trees	KDD-99	- Tree Classifiers - Bayesian Clustering	- Probing - DoS - R2L - U2R	[99]
2008	Giorgio Giacinto *et al.*	Intrusion Detection in Computer Networks by a Modular Ensemble of One-class Classifiers	KDD-99	- Parzen Classifier - v-SVC - k-means	- Probing - DoS - R2L - U2R	[29]
2008	Kaustav Das *et al.*	Anomaly Pattern Detection in Categorical Datasets	1)PIERS 2)Emergency Department Dataset 3)KDD-99	APD - Bayesian Network Likelihood - Conditional Anomaly Detection - WSARE	1) Illegal activity in imported containers 2) Anthrax 3) DoS and R2L	[19]
2008	Weiming Hu *et al.*	AdaBoost-based Algorithm for Network Intrusion Detection	KDD-99	- AdaBoost	- Probing - DoS - R2L - U2R	[41]
2009	Arman Tajbakhsh *et al.*	Intrusion Detection using Fuzzy Association Rules	KDD-99	- ABC - Fuzzy Association Rules	- Probing - DoS - R2L - U2R	[87]
2009	D. Sánchez *et al.*	Association Rules Applied to Credit Card Fraud Detection	Collected transactions dataset	- Fuzzy Association Rules	- Credit Card Fraud	[71]

Continued on next page

Table 3 – *A Decade of Intrusion Detection Systems (2008 - 2018) Continued*

Year	Authors	Paper Title	Dataset	Used Algorithms	Detected Attacks	Ref
2009	Kamran Shafi and Hussein A. Abbass	An Adaptive Genetic-based Signature Learning System for Intrusion Detection	KDD-99	- Genetic-based	- Probing - DoS - R2L - U2R	[74]
2009	Su-Yun Wu and Ester Yen	Data mining-based Intrusion Detectors	KDD-99	- C4.5	- Probing - DoS - R2L - U2R	[98]
2009	Tich Phuoc Tran *et al.*	Novel Intrusion Detection using Probabilistic Neural Network and Adaptive Boosting	KDD-99	BSPNN using: - Adaptive Boosting - Semi-parametric NN	- Probing - DoS - R2L - U2R	[90]
2009	Xiaojun Tong *et al.*	A Research using Hybrid RBF/Elman Neural Networks for Intrusion Detection System Secure Model	1999 DARPA	- RBF - Elman NN	- Probing - DoS - R2L - U2R	[88]
2009	Wei Lu and Hengjian Tong	Detecting Network Anomalies Using CUSUM and EM Clustering	1999 DARPA	- SNORT - Non-Parametric CUSUM - EM based Clustering	13 Attack Types	[57]
2010	Gang Wang *et al.*	A New Approach to Intrusion Detection using Artificial Neural Networks and Fuzzy Clustering	KDD-99	FC-ANN based on: - ANN - Fuzzy Clustering	- Probing - DoS - R2L - U2R	[94]
2010	Min Seok Mok *et al.*	Random Effects Logistic Regression Model for Anomaly Detection	KDD-99	- Logistic Regression	- Probing - DoS - R2L - U2R	[60]

Continued on next page

Table 3 – *A Decade of Intrusion Detection Systems (2008 - 2018) Continued*

Year	**Authors**	**Paper Title**	**Dataset**	**Used Algorithms**	**Detected Attacks**	**Ref**
2010	Muna Mhammad T. Jawhar and Monica Mehrotra	Design Network Intrusion Detection System using hybrid Fuzzy-Neural Network	KDD-99	- NN - FCM Clustering	- Probing - DoS - R2L - U2R	[42]
2011	Cynthia Wagner *et al.*	Machine Learning Approach for IP-Flow Record Anomaly Detection	Generated dataset	- OCSVM	- Nachi scan - Netbios scan - DDoS UDP flood - DDoS TCP flood - stealthy DDoS UDP flood - DDoS UDP flood + traffic deletion Popup spam - SSH scan + TCP flood	[93]
2011	Dewan Md. Farid *et al.*	Adaptive Intrusion Detection based on Boosting and Naive Bayesian Classifier	KDD-99	- AdaBoost - NB	- Probing - DoS - R2L - U2R	[68]
2011	Ming-Yang Su	Real-time Anomaly Detection Systems for Denial-of-Service Attacks by Weighted k-Nearest-Neighbor Classifiers	KDD-99	- Genetic Algorithm - Weighted k-NN	- DoS/DDoS	[84]
2011	Mohammad Saniee Abadeh *et al.*	Design and Analysis of Genetic Fuzzy Systems for Intrusion Detection in Computer Networks	KDD-99	Genetic Fuzzy Systems based on: - Michigan - Pittsburgh - IRL	- Probing - DoS - R2L - U2R	[2]

Continued on next page

Table 3 – *A Decade of Intrusion Detection Systems (2008 - 2018) Continued*

Year	Authors	Paper Title	Dataset	Used Algorithms	Detected Attacks	Ref
2011	Phurivit Sangkatsanee *et al.*	Practical Real-time Intrusion Detection using Machine Learning Approaches	KDD-99	- DT - Ripper Rule - Back-Propagation NN - RBF NN - Bayesian Network - NB	- Probing - DoS	[72]
2011	Seungmin Lee *et al.*	Self-adaptive and Dynamic Clustering for Online Anomaly Detection	KDD-99	- SOM - K-means clustering	- Probing - DoS - R2L - U2R	[51]
2011	Shun-Sheng Wang *et al.*	An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks	KDD-99	- Rule-Based - BON - ART Network	- Probing - DoS - R2L - U2R	[95]
2011	Yang Yi *et al.*	Incremental SVM based on Reserved Set for Network Intrusion Detection	KDD-99	- SVM	- Probing - DoS - R2L - U2R	[102]
2011	Z. Muda *et al.*	Intrusion Detection Based on K-Means Clustering and Naïve Bayes Classification	KDD-99	- K-Means - NB	- Probing - DoS - R2L - U2R	[61]
2012	A.S. Aneetha and S. Bose	The Combined Approach for Anomaly Detection using Neural Networks and Clustering Techniques	KDD-99	- Modified SOM - k-means	- Probing - DoS - R2L - U2R	[8]

Continued on next page

Table 3 – *A Decade of Intrusion Detection Systems (2008 - 2018) Continued*

Year	**Authors**	**Paper Title**	**Dataset**	**Used Algorithms**	**Detected Attacks**	**Ref**
2012	Carlos A. Catania *et al.*	An Autonomous Labeling Approach to Support Vector Machines Algorithms for Network Traffic Anomaly Detection	1998 DARPA	- SVM	- Attack and Non-Attack	[14]
2012	Chi Cheng *et al.*	Extreme Learning Machines for Intrusion Detection	1998 DARPA	ELMs: - Basic - Kernel-Based	- Probing - DoS - R2L - U2R	[16]
2012	Inho Kang *et al.*	A Differentiated One-class Classification Method with Applications to Intrusion Detection	1998 DARPA	- SVDD	- U2R	[44]
2012	Levent Koc *et al.*	A Network Intrusion Detection System Based on a Hidden Naïve Bayes Multiclass Classifier	KDD-99	- Hidden NB	- Probing - DoS - R2L - U2R	[47]
2012	Shih-Wei Lin *et al.*	An Intelligent Algorithm with Feature Selection and Decision Rules Applied to Anomaly Intrusion Detection	KDD-99	- SVM - DT -SA	- Probing - DoS - R2L - U2R	[54]
2012	Siva S. Sivatha Sindhu *et al.*	Decision Tree Based Light Weight Intrusion Detection using a Wrapper Approach	KDD-99	Ensemble DTs: - Decision Stump - C4.5 - NB Tree - Random Forest - Random Tree - Representative Tree model	- Probing - DoS - R2L - U2R	[79]

Continued on next page

Table 3 – *A Decade of Intrusion Detection Systems (2008 - 2018) Continued*

Year	Authors	Paper Title	Dataset	Used Algorithms	Detected Attacks	Ref
2012	Yinhui Li *et al.*	An Efficient Intrusion Detection System based on Support Vector Machines and Gradually Feature Removal Method	KDD-99	- K-means - Ant Colony - SVM	- Probing - DoS - R2L - U2R	[53]
2013	A. M. Chandrashekhar and K. Raghuveer	Fortification of Hybrid Intrusion Detection System using Variants of Neural Networks and Support Vector Machines	KDD-99	- Fuzzy C means - Fuzzy NN / Neurofuzzy - RBF SVM	- Probing - DoS - R2L - U2R	[15]
2013	Dahlia Asyiqin Ahmad Zainaddin and Zurina Mohd Hanapi	Hybrid of Fuzzy Clustering Neural Network over NSL Dataset for Intrusion Detection System	NSL-KDD	- Fuzzy Clustering NN	- Probing - DoS - R2L - U2R	[104]
2013	Mazyar Mohammadi Lisehroodi *et al.*	A Hybrid Framework based on Neural Network MLP and K-means Clustering for Intrusion Detection System	KDD-99	- K-means - NN MLP	- Probing - DoS - R2L - U2R	[56]
2013	S. Devaraju S. Ramakrishnan	Detection of Accuracy for Intrusion Detection System using Neural Network Classifier	KDD-99	- FFNN - ENN - GRNN - PNN - RBNN	- Probing - DoS - R2L - U2R	[21]
2013	Seongjun Shin *et al.*	Advanced Probabilistic Approach for Network Intrusion Forecasting and Detection	DARPA 2000	Advanced Probabilistic Approach for Network-based IDS (APAN) using: - Markov Chain - Kmeans Clustering	- DDoS	[76]
2013	Warusia Yassin *et al.*	Anomaly-based Intrusion Detection Through kmeans Clustering and Naives Bayes Classification	ISCX 2012	- K-Means Clustering and NB Classifier called KMC+NBC	- Normal and Attack	[101]

Continued on next page

Table 3 – *A Decade of Intrusion Detection Systems (2008 - 2018) Continued*

Year	Authors	Paper Title	Dataset	Used Algorithms	Detected Attacks	Ref
2013	Yusuf Sahin *et al.*	A Cost-Sensitive Decision Tree Approach for Fraud Detection	Bank's Credit Card Data	- DT	- Fraud	[70]
2013	Zubair A. Baig *et al.*	GMDH-based Networks for Intelligent Intrusion Detection	KDD-99	Two variants of GMDH: - Monolithic -Ensemble-based	- Probing - DoS - R2L - U2R	[11]
2013	Zubair Md. Fadlullah *et al.*	Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks	Simulated dataset	Non-Parametric CUSUM	- Jamming	[24]
2014	Akhilesh Kumar Shrivas and Amit Kumar Dewangan	An Ensemble Model for Classification of Attacks with Feature Selection based on KDD99 and NSL-KDD Data Set	- KDD-99 - NSL-KDD	ANN-Bayesian Net-GR ensemble: - ANN - Bayesian Net with GR feature selection	- Probing - DoS - R2L - U2R	[78]
2014	Gisung Kim *et al.*	A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection	NSL-KDD	- C4.5 DT - One-class SVM	-	[46]
2014	Ravi Ranjan and G. Sahoo	A New Clustering Approach for Anomaly Intrusion Detection	KDD-99	K-medoids	- Probing - DoS - R2L - U2R	[69]
2014	Wenying Feng *et al.*	Mining Network Data for Intrusion Detection Through Combining SVMs with Ant Colony Networks	KDD-99	- SVM - CSOACN	- Probing - DoS - R2L - U2R	[25]

Continued on next page

Table 3 – *A Decade of Intrusion Detection Systems (2008 - 2018) Continued*

Year	Authors	Paper Title	Dataset	Used Algorithms	Detected Attacks	Ref
2015	Adel Sabry Eesa *et al.*	A Novel Feature-selection Approach based on the Cuttlefish Optimization Algorithm for Intrusion Detection Systems	KDD-99	- DT - Cuttlefish Optimization Algorithm (Feature Selection)	- Probing - DoS - R2L - U2R	[22]
2015	Bisyron Wahyudi Masduki *et al.*	Study on Implementation of Machine Learning Methods Combination for Improving Attacks Detection Accuracy on Intrusion Detection System (IDS)	Reduced sample of GureKddcup: gureKddcup6percent	- SVM	- R2L	[58]
2015	Wei-Chao Lin *et al.*	CANN: An Intrusion Detection System based on Combining Cluster Centers and Nearest Neighbors	KDD-99	- K-means - k-NN	- Probing - DoS - R2L - U2R	[55]
2015	Worachai Srimuang and Silada Intarasothonchun.	Classification Model of Network Intrusion using Weighted Extreme Learning Machine	KDD-99	- Weighted ELM	- Probing - DoS - R2L - U2R	[83]
2016	Amal Hadri *et al.*	Intrusion Detection System using PCA and Fuzzy PCA Techniques	KDD-99	- PCA and Fuzzy PCA - k-NN	- Probing - DoS - R2L - U2R	[31]
2016	Basant Subba *et al.*	Enhancing Performance of Anomaly Based Intrusion Detection Systems through Dimensionality Reduction using Principal Component Analysis	NSL-KDD	- PCA - SVM - MLP - C4.5 - NB	- Probing - DoS - R2L - U2R	[85]

Continued on next page

Table 3 – *A Decade of Intrusion Detection Systems (2008 - 2018) Continued*

Year	**Authors**	**Paper Title**	**Dataset**	**Used Algorithms**	**Detected Attacks**	**Ref**
2016	Elike Hodo *et al.*	Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System	Simulated dataset	- ANN	DoS/DDoS	[37]
2016	Piyush A. Sonewar and Sonali D. Thosar	Detection of SQL Injection and XSS Attacks in Three Tier Web Applications	Generated dataset using httperf	- Mapping	- SQL Injection - XSS	[80]
2016	Praneeth NSKH *et al.*	Principle Component Analysis based Intrusion Detection System Using Support Vector Machine	KDD-99	- SVM - PCA	- Normal and Attack	[63]
2017	Arief Rama Syarif and Windu Gata	Intrusion Detection System using Hybrid Binary PSO and K-Nearest Neighborhood Algorithm	KDD-99	- Binary PSO - k-NN	- Probing - DoS - R2L - U2R	[86]
2017	Binhan Xu *et al.*	Incremental k-NN SVM Method in Intrusion Detection	KDD-99	- R-tree - k-NN - K-means - SVM	- Probing - DoS - R2L - U2R	[100]
2017	Chau Tran *et al.*	HA-IDS: A Heterogeneous Anomaly-based Intrusion Detection System	Generated dataset	- GPU-based ANN - Back-propagation NN	Normal and Attack	[89]
2017	Chuanlong Yin *et al.*	A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks	NSL-KDD	-DL RNN	- Probing - DoS - R2L - U2R	[103]
2017	David Ahmad Effendy *et al.*	Classification of Intrusion Detection System (IDS) Based on Computer Network	NSL-KDD	- K-means - NB - k-means - Information Gain	- Probing - DoS - R2L - U2R	[23]

Continued on next page

Table 3 – *A Decade of Intrusion Detection Systems (2008 - 2018) Continued*

Year	**Authors**	**Paper Title**	**Dataset**	**Used Algorithms**	**Detected Attacks**	**Ref**
2017	Elike Hodo *et al.*	Machine Learning Approach for Detection of nonTor Traffic	UNB-CIC	- ANN - SVM	nonTor Traffic	[39]
2017	Qingru Li *et al.*	An Intrusion Detection System Based on Polynomial Feature Correlation Analysis	KDD-99	- Polynomial Feature Correlation	- DoS	[52]
2017	Shengchu Zhao *et al.*	A Dimension Reduction Model and Classifier for Anomaly-Based Intrusion Detection in Internet of Things	KDD-99	- PCA - Softmax Regression - k-NN	- Probing - DoS - R2L - U2R	[105]
2017	Untari N. Wisesty and Adiwijaya	Comparative Study of Conjugate Gradient to Optimize Learning Process of Neural Network for Intrusion Detection System (IDS)	KDD-99	- Optimized Backpropagation by Conjugate Gradient algorithm (Fletcher Reeves, Polak Ribiere, Powell Beale)	- Probing - DoS - R2L - U2R	[97]
2018	Di He *et al.*	An Improved Kernel Clustering Algorithm Used in Computer Network Intrusion Detection	KDD-99	Kernel Clustering	- Probing - DoS - R2L - U2R	[34]
2018	Mohamad Nazrin Napiah *et al.*	Compression Header Analyzer Intrusion Detection System (CHA - IDS) for 6LoWPAN Communication Protocol	Simulated Dataset	- MLP - SVM - J48 - NB - Logistic - Random Forest Features Selection: - BFS-CFS - GS-CFS	Individual and Combination Routing Attacks: - Hello Flood - Sinkhole - Wormhole	[62]

Continued on next page

Table 3 – *A Decade of Intrusion Detection Systems (2008 - 2018) Continued*

Year	**Authors**	**Paper Title**	**Dataset**	**Used Algorithms**	**Detected Attacks**	**Ref**
2018	Mohammed Hasan Ali *et al.*	A New Intrusion Detection System Based on Fast Learning Network and Particle Swarm Optimization	KDD-99	- FLN - PSO	- Probing - DoS - R2L - U2R	[5]
2018	Muna AL-Hawawreh *et al.*	Identification of Malicious Activities in Industrial Internet of Things based on Deep Learning Models	- NSL-KDD - UNSW-NB15	- Deep Auto-Encoder - ANN	- Probing - DoS - R2L - U2R	[4]
2018	Nathan Shone *et al.*	A Deep Learning Approach to Network Intrusion Detection	- KDD-99 - NSL-KDD	- DL - NDAE - Stacked NDAEs	- Probing - DoS - R2L - U2R	[77]

Where:

* ABC: Association Based Classification
* ANN: Artificial Neural Network
* APD: Anomaly Pattern Detection
* ART: Adaptive Resonance Theory
* BFS-CFS: Best First Search with Correlation Features Selection
* BON: Back-Propagation Network
* BSPNN: Boosted Subspace Probabilistic Neural Network
* CSOACN: Clustering based on Self-Organized Ant Colony Network
* CUSUM: CUmulative SUM
* DL: Deep Learning
* DoS: Denial of Service
* DT: Decision Tree
* ELM: Extreme Learning Machine
* ENN: Elman Neural Network
* FCM: Fuzzy C-Mean
* FFNN: Feed Forward Neural Network
* FLN: Fast Learning Network
* IRL: Iterative Rule Learning
* k-NN: k-Nearest Neighbors
* MLP: Multi-Layer Perceptron
* NB: Naïve Bayes
* NDAE: Non-Symmetric Deep Auto-Encoder
* NN: Neural Network
* OCSVM: One Class Support Vector Machine
* PCA: Principal Component Analysis
* PNN: Probabilistic Neural Network
* PSO: Particle Swarm Optimization
* R2L: Remote to Local
* RBF: Radial Basis Function
* RBNN: Radial Basis Neural Network
* RNN: Recurrent Neural Networks
* SA: Simulated Annealing
* SOM: Self-Organizing Map
* SVDD: Support Vector Data Description

Continued on next page

Table 3 – *A Decade of Intrusion Detection Systems (2008 - 2018) Continued*

Year	Authors	Paper Title	Dataset	Used Algorithms	Detected Attacks	Ref
	* GMDH: Group Method for Data Handling			* SVM: Support Vector Machine		
	* GR: Gain Ratio			* U2R: User to Root		
	* GRNN: Generalized Regression Neural Network			* WSARE: WhatâĂŹs Strange About Recent Events		
	* GS-CFS: Greedy Stepwise with Correlation Features Selection			* XSS: Cross Site Scripting		

Figure 2 shows the distribution of datasets used for research in the last decade. Only 11% of the mentioned IDS used generated or simulated datasets. It is also clear through this analysis that most datasets lack real-life properties which was previously in Section 3.1. Figure 2 also highlights the use of KDD-99 as the dataset of choice. This dataset is deprecated, hence, this demonstrates the inability of the intrusion detection systems presented in Table 3.1 to cope with the most recent attacks.

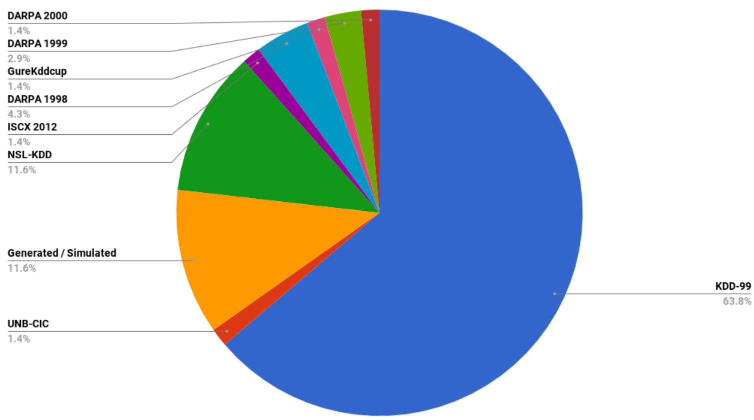


Fig. 2. Distribution of Datasets Used for Evaluation over Discussed IDSs

Figure 3 visualize the attacks detected by the different IDS presented in Table 3.1. It is shown, that the 4 attacks available in the KDD-99 dataset are the most covered, namely; DoS/DDoS, Probing, R2L, U2R.

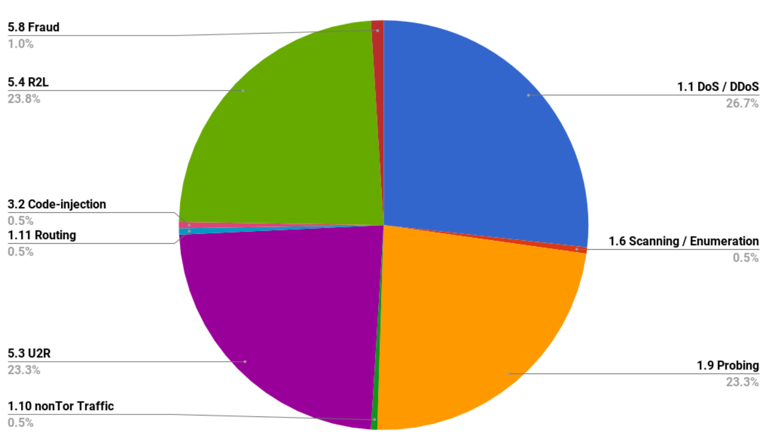
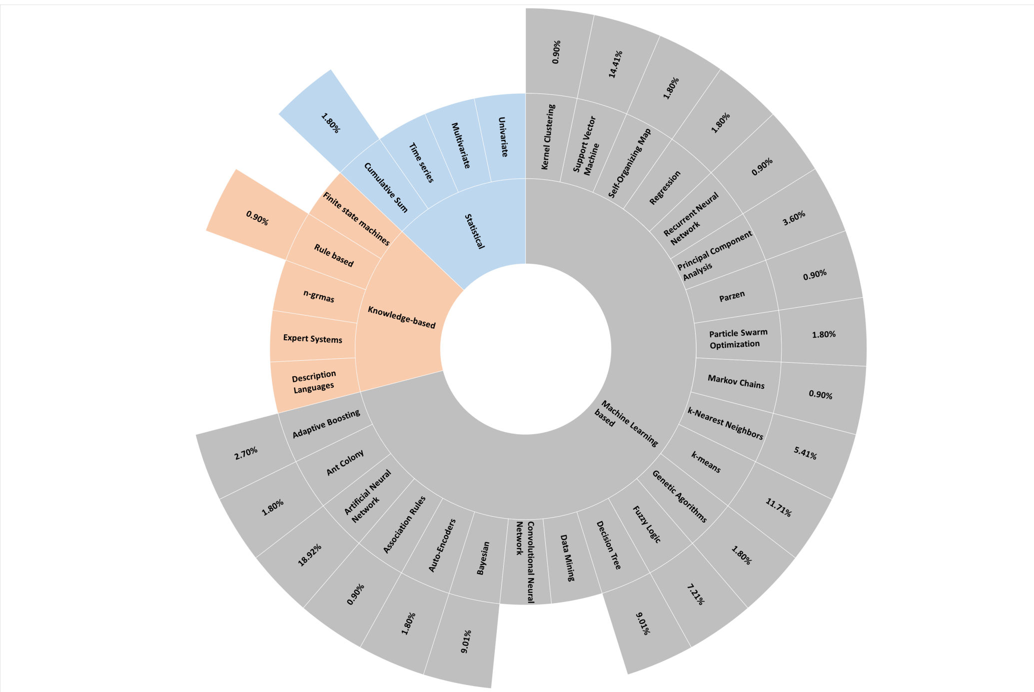


Fig. 3. Covered Attacks in Discussed IDS

Figure 4 (a) highlights the dominance of machine learning algorithms, when building an IDS. As shown, both statistical and knowledge-based algorithms are less represented. Figure 4 (a) is organized by the categories defined in Figure 1 (Inner Circle), The algorithms defined in Figure 1 (4.2.2.2) (Center Circle) and finally the percentage of the IDS presented in Table 3.1 using these algorithms (Outer Circle). Figure 4 (b) on the other hand, provides a visualization of the distribution of the algorithms used by the IDS presented in Table 3.1. It is shown that ANN, SVM and k-means are the most used algorithms overall.



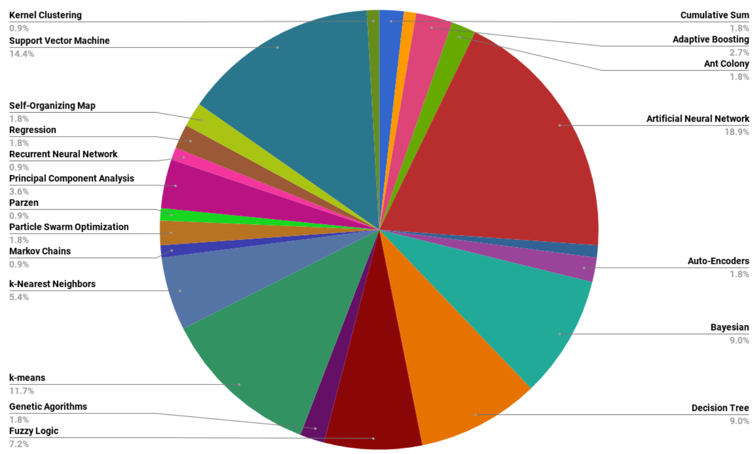
(a) Distribution of all algorithms discussed in Figure 1

4 THREATS TAXONOMY

Building a generic and modular taxonomy for security threats is of high importance in order to help researchers and cyber-security practitioners building tools capable of detecting various attacks ranging from known to 0-day attacks.

Kendall *et al.* [45] proposed one of the earliest classifications of intrusions [92]. Kendall classified intrusions into four categories namely: Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R) and Probing. In DoS, the attacker tend to prevent users from accessing a given service. When the attacker tried to gain authorized access to the target system, either by gaining a local access or promoting the user to a root user, these attacks were classified as R2L and U2R respectively. Finally, probing was defined, by an attacker actively foot printing a system for vulnerabilities.

Donald Welch classified the common threats in wireless networks into seven attack techniques (Traffic Analysis, Passive Eavesdropping, Active Eavesdropping, Unauthorized Access, Man-in-the-middle, Session High-Jacking and Replay) [96]. In a paper by Sachin Babar *et al.* [10], the problem is addressed from a different perspective. Threats are classified according to the Internet of things security requirements (identification, communication, physical threat, embedded security and storage management). Specific domain taxonomies have also grabbed the attention of researchers. David Kotz [48] discusses privacy threats in mobile health (mHealth) domain. In the same manner,



(b) Distribution of used algorithms discussed in Table 3.1

Fig. 4. Algorithms usage distribution in the discussed IDSs

Keshnee Padayachee [64], shows the security threats targeting compliant information and Monjur Ahmed and Alan T. Litchfield [3] works on threats from a cloud computing point of view.

This Section classifies network threats based on the layers of the OSI model, provides examples of attacks for different threat types and provides a taxonomy associating network threats and the tools used to carry out attacks. The taxonomies aim at helping researchers building IDS, but more importantly by associating the threats to the OSI model, as well as the threats to the tools used to carry attack or take advantage of specific vulnerabilities, the taxonomies aim at achieving higher accuracies and reducing the amount of false positives of current intrusion detection systems [77] as well as building better datasets.

4.1 Threat Sources

Figure 5 identify network threats and provides a classification according to the following criteria (I) Source of the threat, (II) Affected layer based on Open Systems Interconnection (OSI) model and (III) Active and Passive threats. The different threats are described hereafter (Note that the taxonomy is available through a a Github repository for public access and contributions [1].

As shown, attacks can be targeting a single layer of the OSI model, but it is important to highlight that other layers may also be affected. The taxonomy presented in this manuscript focus on the main target layer of attack. An attack is also described to be active if it affects information, performance or any aspect of the media on which it is running. In contrast to active attacks, during passive attacks the attacker is concerned with either gathering information or monitoring the network. These can be identified by their shape in Figure 5. Active attacks are represented by a *rectangle shape*, while passive attacks are represented by an *oval shape*. Attacks like adware (2.1.3), spyware (2.1.4) and information gathering (3.1) are considered passive attacks. DoS (1.1), Impersonation (1.4) and Virus (2.1.2) are forms of active attacks. However, some attacks cannot be considered active or passive until their usage is known. An example of this case are SQL-injections, if it is used for

[1]https://github.com/AbertayMachineLearningGroup/network-threats-taxonomy

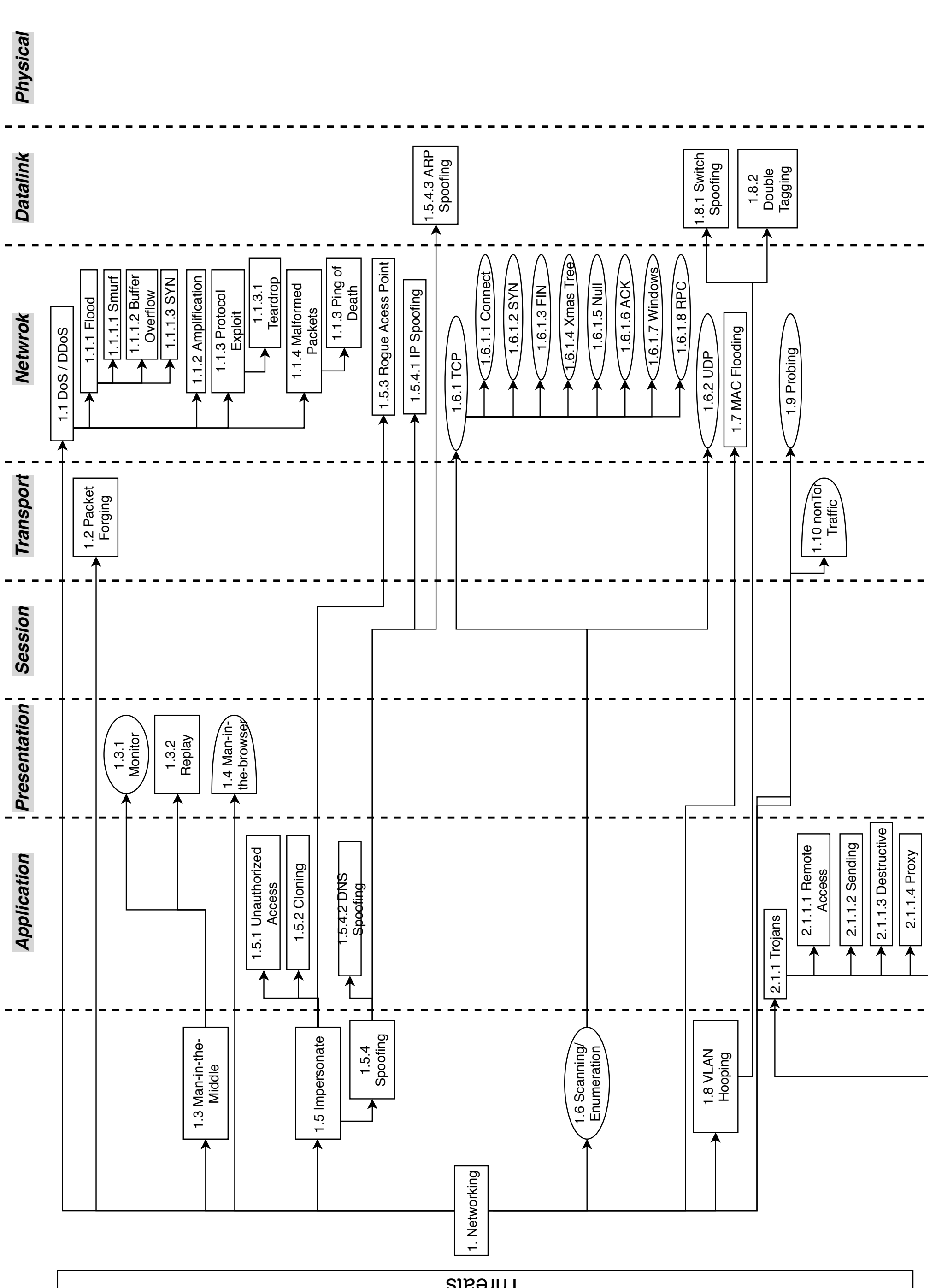


Fig. 5. Taxonomy of threats (1 of 2)

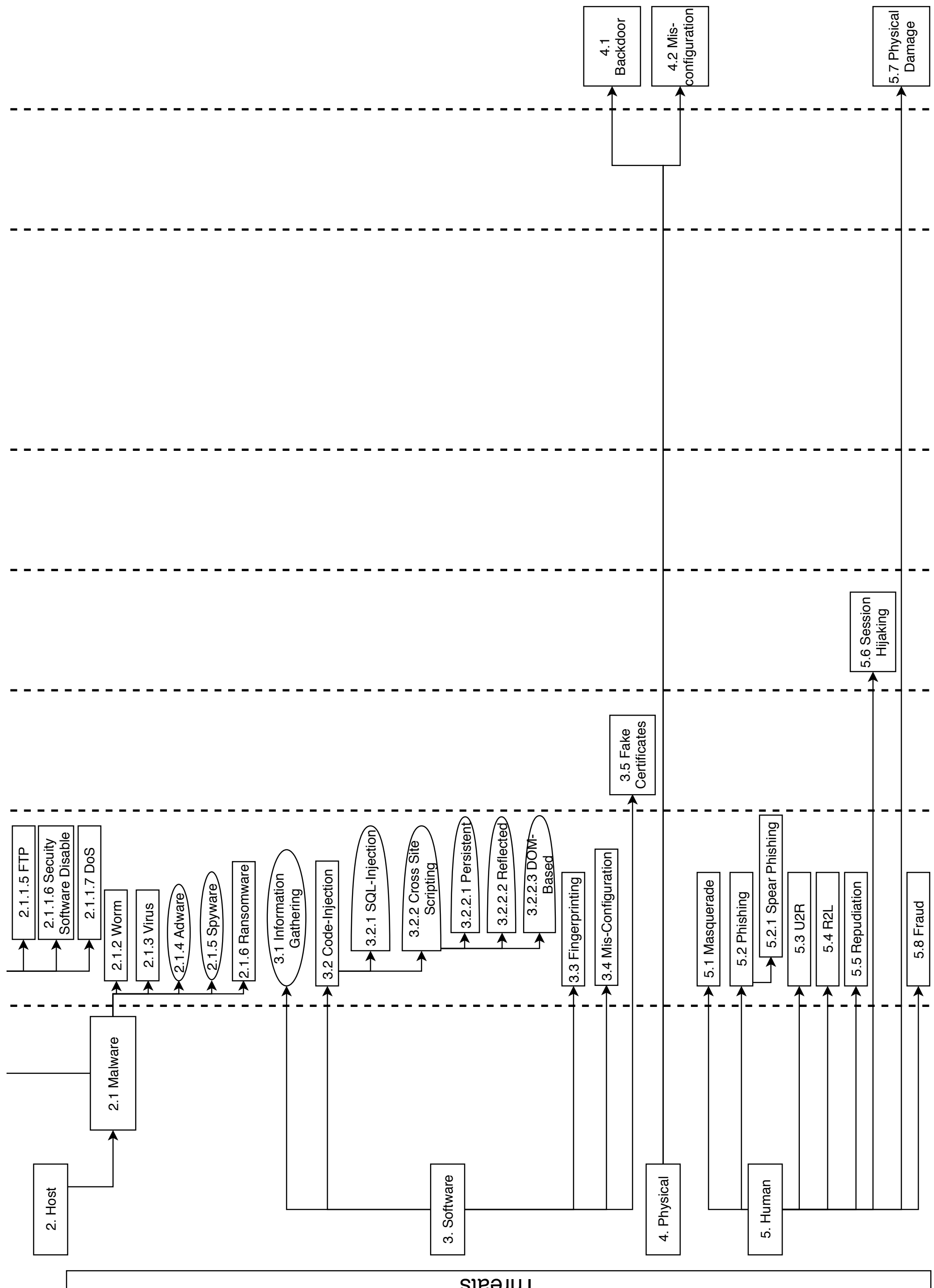


Fig. 5. Taxonomy of threats (2 of 2)

querying data from a database then it is passive. However, if it is used to alter data, drop tables or relations then the attack can be considered as active.

4.1.1 Network Threats. Threats are initiated based on a flow of packet sent over a network. Two of the most common forms of network threats are Denial of Service (DoS) and Distributed Denial of Service (DDoS) (1.1) where an attacker floods the network with requests rendering the service unresponsive. During Attacks legitimate users cannot access the services. Note that common anomalies known as 'Flash Crowds' are often mistaken with DoS and DDoS attacks [43]. Dos and DDoS can be divided in four categories including flood attacks (1.1.1), amplification attacks (1.1.2), protocol exploit (1.1.3), and malformed packets (1.1.4). These are defined respectively through attack examples. Smurf attacks (1.1.1.1) depends on generating a large amount of ping requests. Overflows (1.1.1.2) occurs when a program writes more bytes than allowed. This occurs when an attacker sends packets larger than 65536 bytes (allowed in the IP protocol) and the stack does not have an appropriate input sanitation in place. The ping of Death (1.1.4.1) attack occurs when packets are too large for the routers and splitting is required. The Teardrop (1.1.3.1) attack takes place when an incorrect offset is set by the attacker. Finally the SYN flood (1.1.1.3) attack happens when the host allocates memory for a huge number of TCP SYN packets.

Packet forging (1.2) is another form of networking attack. Packet forging or injection is the action in which the attacker generates packets that look the same as those of the network. These packets can be used to perform certain action, steal information, etc. When the attacker intercepts communications between two or more entities and starts to either control the communication between them and alter the communication or listen to the network, this attack is referred to as a 'Man in the Middle' attack (1.3). Unlike 'Man in the Middle' attack, a 'Man In The Browser' attack (1.4) intercepts the browser to alter or add fields to a web page asking the user to enter confidential data. Impersonation (1.5) or pretending to be another user can take different forms. The attacker may impersonate a user to gain higher security level and gain access to unauthorized data (1.5.1) or use cloned accounts, cloning (1.5.2) is common in social networks. Another impersonation form in wireless networks are rogue access points (1.5.3). During an IP spoofing (1.5.4.1) attack an attacker spoofs an IP address and sends packets impersonating a legitimate host. DNS spoofing - also known as DNS cache poisoning - (1.5.4.2) is another type of spoofing. The attacker redirects packets by poisoning the DNS. Finally, ARP spoofing (1.5.4.3) is used to perform attack like Man In the Middle, in order to dissociate legitimate IP and MAC addresses in the ARP tables of the victims.

Scanning/enumeration are an essential step for initiating attacks. During scanning (1.6), the attacker starts with searching the network for information such as, active nodes, the running operating system, software versions, etc. As defined in [59], scanning has many forms,using protocols such as TCP (1.6.1) or UDP (1.6.2). The last two examples of network attacks are media access control (MAC) address flooding (1.7), and VLAN hopping attack (1.8). In MAC flooding (1.7), the attacker is targeting the network switches and as a result, packets are redirected to the wrong physical ports, while the VLAN hopping attack has two forms either switch spoofing (1.8.1) or double tagging (1.8.2).

4.1.2 Host Threats. Host attacks target specific hosts or system by running malicious software to compromise the system functionalities or corrupt it. Most host attacks are categorized under the malware (2.1) category. This includes worms, viruses, adwares, spywares, Trojans and ransomware. Viruses are known to affect programs and files when shared with other users on the network while worms are known to self-replicate affecting multiple systems. Adwares are known for showing advertisements to users when surfing the Internet or installing software. Although adware are less likely to run malicious code, it can compromise the performance of a system. Spyware, gathers information such as documents, user cookies, browsing history, emails, etc. or monitor and track user actions. Trojans often look like trusted applications, but allow the attacker to control the device. Last, ransomware are a relatively new type of malware where the system is kept under the control of the attacker - or a third entity - by encrypting the files until the user/organization pay a ransom [1].

4.1.3 Software Threats. Code injection (3.2) can include SQL Injection to query the database, resulting in obtaining confidential data, or deleting data by dropping columns, rows or tables. Cross-site scripting (XSS) is used to run malicious code to steal cookies or credentials. XSS have three main categories. The first is persistent/stored XSS (3.2.2.1), in this case the script is saved in the database and is executed every time the page is loaded. The second is Reflected XSS (3.2.2.2) in which the script is part of the HTTP requests sent to the server. The last is DOM-based XSS (3.2.2.3) which can be considered as an advanced type of XSS. The attacker changes values in the Document Object Model (DOM) e.g. document location, document url, etc. DOM-based XSS are difficult to detect as the script is never transferred to the server. Fingerprinting and misconfiguration are also forms of software threats. Fake server certificates (3.5) should be considered while building web applications or analysing communications.

4.1.4 Physical Threats. Physical attacks are a result of a tempering attempt on the network hardware (edge, or other devices) or its configuration. This can include changing the configurations (4.2) and to introducing backdoors (i.e. The Evil Maid).

4.1.5 Human Threats. The last category of networking attacks are the one based on human actions. These includes user masquerade (5.1). Phishing is another form of human attacks in which the attacker uses emails or other electronic messaging services to obtain credentials or confidential data. When a user attempts to take higher privileges it is considered a human attack like User to Root (5.3) and Remote to Local R2L (5.4). Additionally, a user can be denied an action such as repudiation (5.5) attack. Human attacks can also include session hijacking or sniffing,these attacks are based on the attacker gaining access over an active session to access to cookies and tokens.

Fig. 6. Distribution of Covered Attacks in Discussed IDSs

Based on the taxonomy discussed in Figure 5 and the recent IDS in Table 3, it can be seen that there are many threats that are not addressed by recent IDS. Figure 6 visualize all the threats mentioned in the taxonomy. The associated percentage represents the the attacks covered by the IDS discussed in Section 3.1, Table 3.1. As shown a large number of attacks are not covered.

4.2 Attacking Tools

Many tools [59] [40] have been developed to initiate different attacks. Figure 7 show the main tools classified by the attacks they are used for. This can be used by researchers when building an IDS for a specific threat, then the associated tools are the ones of interest. For example, for an IDS classifying impersonation attacks, Caffe-Latte, Hirte, EvilTwin and Cain and Abel are the ones to check. Yaga and SQL attack are used for U2R and so on.

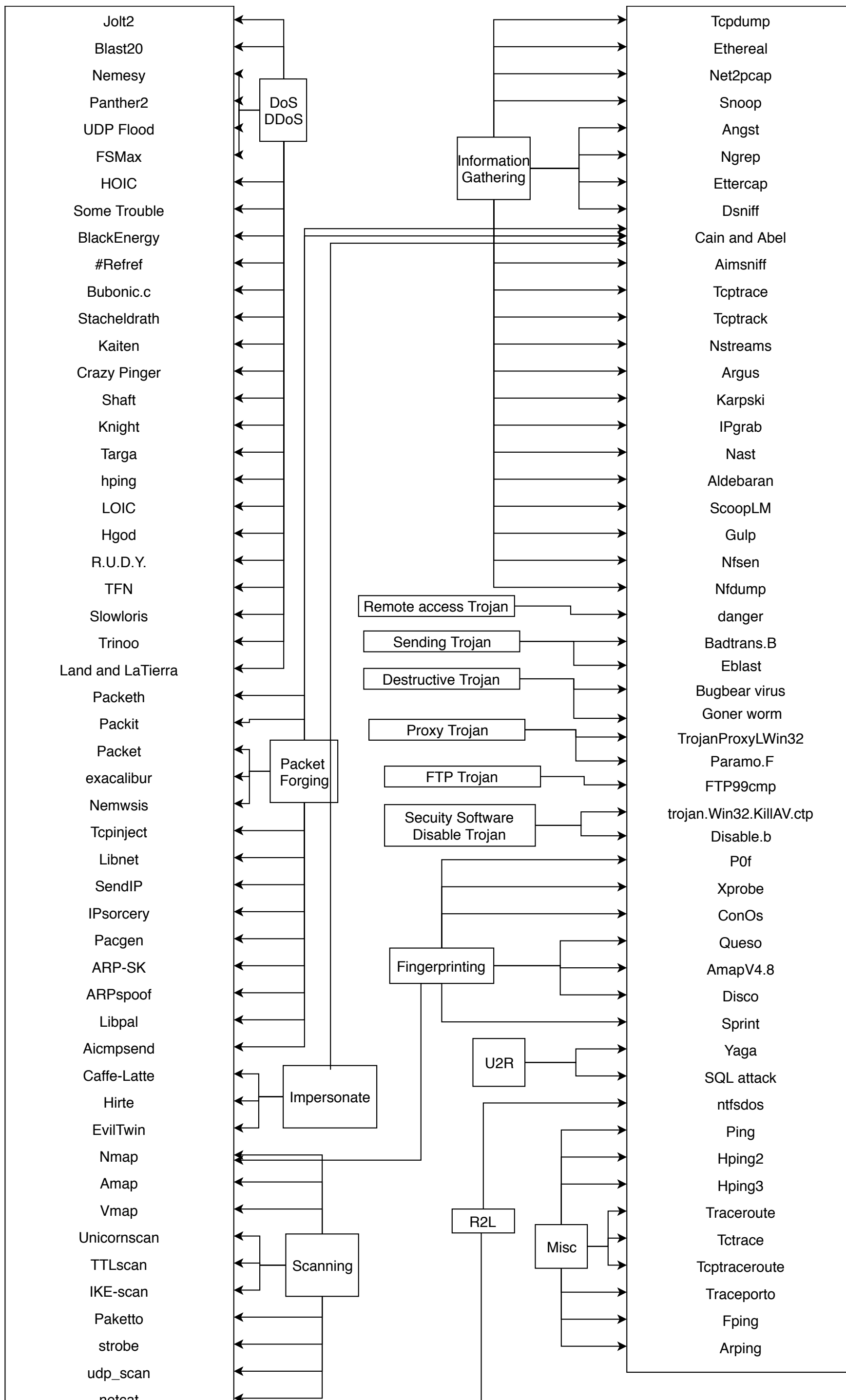


Fig. 7. Attacks Tools Example

5 CONCLUSION

This manuscript aims at providing an overview of intrusion detection system internals, the way they are expected to work, as well as evaluation criteria and classifications problems. Furthermore, the manuscript tackles the problem of having a generic taxonomy for network threats. A proposed taxonomy is presented for categorizing network attacks based on the source, OSI model layer and whether the threat is active or passive. The prominent IDS research of the past decade (2008 - 2018) are analyzed. The analysis results in three main findings. Benchmark datasets lack real world property and fail to cope with the constant changes in attacks and networks architectures.

Moreover, we present a taxonomy of tools and associated attacks, and demonstrate the current IDS research only cover around 25% of the threats presented in the taxonomy. Furthermore we highlight that, while machine learning is used by 97.25% of the surveyed IDS. ANN, k-means and SVM represent the majority of the algorithms used. While these algorithms present outstanding results, we also highlight that these results are obtained on outdated datasets and hence, not representative of real-world architectures and attack scenarios.

Finally, the network threat taxonomy and the attacks and associated tool taxonomy are open-sourced and available through Github, allowing both securiry and acdemic researchers to contribute to the taxonomy and ensure its relevance in the future[2].

[2]https://github.com/AbertayMachineLearningGroup/network-threats-taxonomy

REFERENCES

[1] 2018. Malware vs Viruses: What's the Difference? (February 2018). https://antivirus.comodo.com/blog/computer-safety/malware-vs-viruses-whats-difference/ (Accessed on 02/28/2018).

[2] Mohammad Saniee Abadeh, Hamid Mohamadi, and Jafar Habibi. 2011. Design and analysis of genetic fuzzy systems for intrusion detection in computer networks. (2011), 7067-7075 pages. https://doi.org///doi.org/10.1016/j.eswa.2010.12.006 ID: 271506.

[3] Monjur Ahmed and Alan T Litchfield. 2018. Taxonomy for identification of security issues in cloud computing environments. Journal of Computer Information Systems 58, 1 (2018), 79–88.

[4] Muna AL-Hawawreh, Nour Moustafa, and Elena Sitnikova. 2018. Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications 41 (2018), 1–11. https://doi.org///doi.org/10.1016/j.jisa.2018.05.002 ID: 287016.

[5] Mohammed Hasan Ali, Bahaa Abbas Dawood AL Mohammed, Madya Alyani Binti Ismail, and Mohamad Fadli Zolkipli. 2018. A new intrusion detection system based on Fast Learning Network and Particle swarm optimization. IEEE Access 6 (2018), 20255–20261.

[6] Suhair Hafez Amer and J Hamilton. 2010. Intrusion detection systems (IDS) taxonomy-a short review. Defense Cyber Security 13, 2 (2010), 23–30.

[7] Muhamad Erza Aminanto, Rakyong Choi, Harry Chandra Tanuwidjaja, Paul D. Yoo, and Kwangjo Kim. 2018. Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection. IEEE Transactions on Information Forensics and Security 13, 3 (2018), 621–636.

[8] A. S. Aneetha and S. Bose. 2012. The combined approach for anomaly detection using neural networks and clustering techniques. Computer Science and Engineering 2, 4 (2012), 37–46.

[9] Buse Atli. 2017. Anomaly-Based Intrusion Detection by Modeling Probability Distributions of Flow Characteristics. Ph.D. Dissertation. School of Electrical Engineering, Aalto University. http://urn.fi/URN:NBN:fi:aalto-201710307348[urn]

[10] Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad. 2010. Proposed security model and threat taxonomy for the Internet of Things (IoT). In International Conference on Network Security and Applications. Springer, 420–429.

[11] Zubair A. Baig, Sadiq M. Sait, and AbdulRahman Shaheen. 2013. GMDH-based networks for intelligent intrusion detection. (2013), 1731-1740 pages. https://doi.org///doi.org/10.1016/j.engappai.2013.03.008 ID: 271095.

[12] Xavier JA Bellekens, Christos Tachtatzis, Robert C Atkinson, Craig Renfrew, and Tony Kirkham. 2014. Glop: Enabling massively parallel incident response through gpu log processing. In Proceedings of the 7th International Conference on Security of Information and Networks. ACM, 295.

[13] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar. 2014. A Survey of Intrusion Detection Systems in Wireless Sensor Networks. IEEE Communications Surveys & Tutorials 16, 1 (2014), 266–282. https://doi.org/10.1109/SURV.2013.050113.00191

[14] Carlos A. Catania, Facundo Bromberg, and Carlos GarcÃŋa Garino. 2012. An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection. (2012), 1822-1829 pages. https://doi.org///doi.org/10.1016/j.eswa.2011.08.068 ID: 271506.

[15] A. M. Chandrashekhar and K. Raghuveer. 2013. Fortification of hybrid intrusion detection system using variants of neural networks and support vector machines. International Journal of Network Security and Its Applications 5, 1 (2013), 71–90.

[16] Chi Cheng, Wee Peng Tay, and Guang-Bin Huang. 2012. Extreme learning machines for intrusion detection. In Neural networks (IJCNN), the 2012 international joint conference on. IEEE, 1–8.

[17] Cisco. 2017. Cisco Visual Networking Index: Forecast and Methodology, 2016-2021. (Sep 2017). https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html (Accessed on 02/15/2018).

[18] Gideon Creech and Jiankun Hu. 2013. Generation of a new IDS test dataset: Time to retire the KDD collection. In Wireless Communications and Networking Conference (WCNC), 2013 IEEE. IEEE, 4487–4492.

[19] Kaustav Das, Jeff Schneider, and Daniel B. Neill. 2008. Anomaly pattern detection in categorical datasets. In Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 169–176.

[20] Hervé Debar, Marc Dacier, and Andreas Wespi. 1999. Towards a taxonomy of intrusion-detection systems. Computer Networks 31, 8 (1999), 805–822.

[21] S. Devaraju and S. Ramakrishnan. 2013. Detection of accuracy for intrusion detection system using neural network classifier. International Journal of Emerging Technology and Advanced Engineering 3, 1 (2013), 338–345.

[22] Adel Sabry Eesa, Zeynep Orman, and Adnan Mohsin Abdulazeez Brifcani. 2015. A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems. (2015), 2670-2679 pages. https://doi.org///doi.org/10.1016/j.eswa.2014.11.009 ID: 271506.

[23] David Ahmad Effendy, Kusrini Kusrini, and Sudarmawan Sudarmawan. 2017. Classification of intrusion detection system (IDS) based on computer network. In Proceedings of 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE). IEEE, 90–94.

[24] Zubair Md Fadlullah, Hiroki Nishiyama, Nei Kato, and Mostafa M. Fouda. 2013. Intrusion detection system (IDS) for combating attacks against cognitive radio networks. IEEE Network 27, 3 (2013), 51–56.

[25] Wenying Feng, Qinglei Zhang, Gongzhu Hu, and Jimmy Xiangji Huang. 2014. Mining network data for intrusion detection through combining SVMs with ant colony networks. (2014), 127-140 pages. https://doi.org///doi.org/10.1016/j.future.2013.06.027 ID: 271521.

[26] Center for Applied Internet Data Analysis. [n. d.]. CAIDA Data. ([n. d.]). http://www.caida.org/data/index.xml

[27] Canadian Institute for Cybersecurity. [n. d.]. Intrusion detection evaluation dataset (ISCXIDS2012). ([n. d.]). http://www.unb.ca/cic/datasets/ids.html

[28] Seyed Mohammad Ghaffarian and Hamid Reza Shahriari. 2017. Software Vulnerability Analysis and Discovery Using Machine-Learning and Data-Mining Techniques: A Survey. ACM Computing Surveys (CSUR) 50, 4 (2017), 56.

[29] Giorgio Giacinto, Roberto Perdisci, Mauro Del Rio, and Fabio Roli. 2008. Intrusion detection in computer networks by a modular ensemble of one-class classifiers. (2008), 69-82 pages. https://doi.org///doi.org/10.1016/j.inffus.2006.10.002 ID: 272144.

[30] The Shmoo Group. 2000. DEFCON 8, 10 and 11. (2000). http://cctf.shmoo.com/

[31] Amal Hadri, Khalid Chougdali, and Rajae Touahni. 2016. Intrusion detection system using PCA and Fuzzy PCA techniques. In Advanced Communication Systems and Information Security (ACOSIS), International Conference on. IEEE, 1–7.

[32] Tarfa Hamed, Jason B Ernst, and Stefan C Kremer. 2018. A Survey and Taxonomy of Classifiers of Intrusion Detection Systems. In Computer and Network Security Essentials. Springer, 21–39.

[33] Julie Hamon. 2013. Combinatorial optimization for variable selection in high dimensional regression: Application in animal geneti Ph.D. Dissertation. Université des Sciences et Technologie de Lille - Lille I. https://tel.archives-ouvertes.fr/tel-00920205

[34] Di He, Xin Chen, Danping Zou, Ling Pei, and Lingge Jiang. 2018. An Improved Kernel Clustering Algorithm Used in Computer Network Intrusion Detection. 1–5. https://doi.org/10.1109/ISCAS.2018.8350994

[35] Jose Crispin Hernandez Hernandez, Béatrice Duval, and Jin-Kao Hao. 2007. A genetic embedded approach for gene selection and classification of microarray data. In European Conference on Evolutionary Computation, Machine Learning and Data Mining in Bioinformatics. Springer, 90–101.

[36] S. Hettich and S. D. Bay. 1999. The UCI KDD Archive. (1999). http://kdd.ics.uci.edu

[37] Elike Hodo, Xavier Bellekens, Andrew Hamilton, Pierre-Louis Dubouilh, Ephraim Iorkyase, Christos Tachtatzis, and Robert Atkinson. 2016. Threat analysis of IoT networks using artificial neural network intrusion detection system. In 2016 International Symposium on Networks, Computers and Communications (IEEE ISNCC'16). IEEE, 1–6.

[38] Elike Hodo, Xavier Bellekens, Andrew Hamilton, Christos Tachtatzis, and Robert Atkinson. 2017. Shallow and deep networks intrusion detection system: A taxonomy and survey. arXiv preprint arXiv:1701.02145 (2017), 1–43.

[39] Elike Hodo, Xavier Bellekens, Ephraim Iorkyase, Andrew Hamilton, Christos Tachtatzis, and Robert Atkinson. 2017. Machine Learning Approach for Detection of nonTor Traffic. ACM, Reggio Calabria, Italy, 1–6.

[40] Nazrul Hoque, Monowar H. Bhuyan, Ram Charan Baishya, Dhruba K. Bhattacharyya, and Jugal K. Kalita. 2014. Network attacks: Taxonomy, tools and systems. Journal of Network and Computer Applications 40 (2014), 307–324. https://doi.org///doi.org/10.1016/j.jnca.2013.08.001 ID: 272436.

[41] W. Hu, W. Hu, and S. Maybank. 2008. AdaBoost-based algorithm for network intrusion detection. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics 38, 2 (2008), 577–583. https://doi.org/10.1109/TSMCB.2007.914695 Cited By :137.

[42] Muna Mhammad T. Jawhar and Monica Mehrotra. 2010. Design network intrusion detection system using hybrid fuzzy-neural network. International Journal of Computer Science and Security 4, 3 (2010), 285–294.

[43] Jaeyeon Jung, Balachander Krishnamurthy, and Michael Rabinovich. 2002. Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites. In Proceedings of the 11th international conference on World Wide Web. ACM, 293–304.

[44] Inho Kang, Myong K. Jeong, and Dongjoon Kong. 2012. A differentiated one-class classification method with applications to intrusion detection. (2012), 3899-3905 pages. https://doi.org///doi.org/10.1016/j.eswa.2011.06.033 ID: 271506.

[45] Kristopher Kristopher Robert Kendall. 1999. A database of computer attacks for the evaluation of intrusion detection systems. Ph.D. Dissertation.

[46] Gisung Kim, Seungmin Lee, and Sehun Kim. 2014. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. (2014), 1690-1700 pages. https://doi.org///doi.org/10.1016/j.eswa.2013.08.066 ID: 271506.

[47] Levent Koc, Thomas A. Mazzuchi, and Shahram Sarkani. 2012. A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier. (2012), 13492-13500 pages. https://doi.org///doi.org/10.1016/j.eswa.2012.07.009 ID: 271506.

[48] David Kotz. 2011. A threat taxonomy for mHealth privacy. In Communication Systems and Networks (COMSNETS), 2011 Third International Conference on. IEEE, 1–6.

[49] Lincoln Laboratory. [n. d.]. MIT Lincoln Laboratory: DARPA Intrusion Detection Evaluation. ([n. d.]). https://www.ll.mit.edu/ideval/data

[50] (LBNL) Lawrence Berkeley National Laboratory and (ICSI) International Computer Science Institute. 2005. LBNL/ICSI Enterprise Tracing Project. (2005). http://www.icir.org/enterprise-tracing/Overview.html

[51] Seungmin Lee, Gisung Kim, and Sehun Kim. 2011. Self-adaptive and dynamic clustering for online anomaly detection. (2011), 14891-14898 pages. https://doi.org///doi.org/10.1016/j.eswa.2011.05.058 ID: 271506.

[52] Qingru Li, Zhiyuan Tan, Aruna Jamdagni, Priyadarsi Nanda, Xiangjian He, and Wei Han. 2017. An intrusion detection system based on polynomial feature correlation analysis. In Trustcom/BigDataSE/ICESS, 2017 IEEE. IEEE, 978–983.

[53] Yinhui Li, Jingbo Xia, Silan Zhang, Jiakai Yan, Xiaochuan Ai, and Kuobin Dai. 2012. An efficient intrusion detection system based on support vector machines and gradually feature removal method. (2012), 424-430 pages. https://doi.org///doi.org/10.1016/j.eswa.2011.07.032 ID: 271506.

[54] Shih-Wei Lin, Kuo-Ching Ying, Chou-Yuan Lee, and Zne-Jung Lee. 2012. An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection. (2012), 3285-3290 pages. https://doi.org///doi.org/10.1016/j.asoc.2012.05.004 ID: 272229.

[55] Wei-Chao Lin, Shih-Wen Ke, and Chih-Fong Tsai. 2015. CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. (2015), 13-21 pages. https://doi.org///doi.org/10.1016/j.knosys.2015.01.009 ID: 271505.

[56] Mazyar Mohammadi Lisehroodi, Zaiton Muda, and Warusia Yassin. 2013. A hybrid framework based on neural network MLP and K-means Clustering for Intrusion Detection System. In Proceedings of 4th International Conference on Computing and Informatics, ICOCI. 305–311.

[57] Wei Lu and Hengjian Tong. 2009. Detecting network anomalies using CUSUM and EM clustering. In International Symposium on Intelligence Computation and Applications. Springer, 297–308.

[58] Bisyron Wahyudi Masduki, Kalamullah Ramli, Ferry Astika Saputra, and Dedy Sugiarto. 2015. Study on implementation of machine learning methods combination for improving attacks detection accuracy on Intrusion Detection System (IDS). In Quality in Research (QiR), 2015 International Conference on. IEEE, 56–64.

[59] Stuart McClure, Joel Scambray, and George Kurtz. 2009. Hacking Exposed: Network Security Secrets and Solutions, Sixth Edition. McGraw-Hill Osborne Media. https://www.amazon.com/Hacking-Exposed-Network-Security-Solutions/dp/0071613749?SubscriptionId=0JYN1NVW651KCA56C102&tag=techkie-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=0071613749

[60] Min Seok Mok, So Young Sohn, and Yong Han Ju. 2010. Random effects logistic regression model for anomaly detection. (2010), 7162-7166 pages. https://doi.org///doi.org/10.1016/j.eswa.2010.04.017 ID: 271506.

[61] Z. Muda, W. Yassin, M. N. Sulaiman, and N. I. Udzir. 2011. A K-Means and Naive Bayes learning approach for better intrusion detection. Information technology journal 10, 3 (2011), 648–655.

[62] Mohamad Nazrin Napiah, Mohd Yamani Idna Idris, Roziana Ramli, and Ismail Ahmedy. 2018. Compression Header Analyzer Intrusion Detection System (CHA-IDS) for 6LoWPAN Communication Protocol. IEEE Access 6 (2018), 16623–16638.

[63] Praneeth Nskh, M. Naveen Varma, and Roshan Ramakrishna Naik. 2016. Principle component analysis based intrusion detection system using support vector machine. In Recent Trends in Electronics, Information and Communication Technology (RTEICT), IEEE International Conference on. IEEE, 1344–1350.

[64] Keshnee Padayachee. 2012. Taxonomy of compliant information security behavior. Computers & Security 31, 5 (2012), 673–680.

[65] Tu Minh Phuong, Zhen Lin, and Russ B Altman. 2005. Choosing SNPs using feature selection. In Computational Systems Bioinformatics Conference, 2005. Proceedings. 2005 IEEE. IEEE, 301–309.

[66] R. Senthil Prabha and R. Vidhyapriya. 2017. Intruder Detection System Based on Behavioral Biometric Security. Journal of Scientific & Industrial Research 76 (2017), 90–94.

[67] Swagatika Prusty, Brian Neil Levine, and Marc Liberatore. 2011. Forensic investigation of the OneSwarm anonymous filesharing system. In Proceedings of the 18th ACM conference on Computer and communications security. ACM, 201–214.

[68] Chowdhury Mofizur Rahman, Dewan Md Farid, and Mohammad Zahidur Rahman. 2011. Adaptive intrusion detection based on boosting and naive bayesian classifier. International Journal of Computer Applications 24, 3 (2011), 11–19.

[69] Ravi Ranjan and G. Sahoo. 2014. A new clustering approach for anomaly intrusion detection. arXiv preprint arXiv:1404.2772 4, 2 (2014), 29–38.

[70] Yusuf Sahin, Serol Bulkan, and Ekrem Duman. 2013. A cost-sensitive decision tree approach for fraud detection. (2013), 5916-5923 pages. https://doi.org///doi.org/10.1016/j.eswa.2013.05.021 ID: 271506.

[71] D. Sánchez, M. A. Vila, L. Cerda, and J. M. Serrano. 2009. Association rules applied to credit card fraud detection. (2009), 3630-3640 pages. https://doi.org///doi.org/10.1016/j.eswa.2008.02.001 ID: 271506.

[72] Phurivit Sangkatsanee, Naruemon Wattanapongsakorn, and Chalermpol Charnsripinyo. 2011. Practical real-time intrusion detection using machine learning approaches. (2011), 2227-2235 pages. https://doi.org///doi.org/10.1016/j.comcom.2011.07.001 ID: 271515.

[73] Benjamin Sangster, T. J. O'Connor, Thomas Cook, Robert Fanelli, Erik Dean, Christopher Morrell, and Gregory J. Conti. 2009. Toward Instrumenting Network Warfare Competitions to Generate Labeled Datasets.. In CSET. Berkeley, CA: Usenix, The Advanced Computing System Association).

[74] Kamran Shafi and Hussein A. Abbass. 2009. An adaptive genetic-based signature learning system for intrusion detection. (2009), 12036-12043 pages. https://doi.org///doi.org/10.1016/j.eswa.2009.03.036 ID: 271506.

[75] Iman Sharafaldin, Amirhossein Gharib, Arash Habibi Lashkari, and Ali A Ghorbani. 2018. Towards a Reliable Intrusion Detection Benchmark Dataset. Software Networking 2018, 1 (2018), 177–200.

[76] Seongjun Shin, Seungmin Lee, Hyunwoo Kim, and Sehun Kim. 2013. Advanced probabilistic approach for network intrusion forecasting and detection. (2013), 315-322 pages. https://doi.org///doi.org/10.1016/j.eswa.2012.07.057 ID: 271506.

[77] Nathan Shone, Tran Nguyen Ngoc, Vu Dinh Phai, and Qi Shi. 2018. A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence 2, 1 (2018), 41–50.

[78] Akhilesh Kumar Shrivas and Amit Kumar Dewangan. 2014. An ensemble model for classification of attacks with feature selection based on KDD99 and NSL-KDD data set. International Journal of Computer Applications 99, 15 (2014), 8–13.

[79] Siva S. Sivatha Sindhu, S. Geetha, and A. Kannan. 2012. Decision tree based light weight intrusion detection using a wrapper approach. (2012), 129-141 pages. https://doi.org///doi.org/10.1016/j.eswa.2011.06.013 ID: 271506.

[80] Piyush A. Sonewar and Sonali D. Thosar. 2016. Detection of SQL injection and XSS attacks in three tier web applications. In Computing Communication Control and automation (ICCUBEA), 2016 International Conference on. IEEE, 1–4.

[81] Jungsuk Song, Hiroki Takakura, Yasuo Okabe, Masashi Eto, Daisuke Inoue, and Koji Nakao. 2011. Statistical analysis of honeypot data and building of Kyoto 2006 dataset for NIDS evaluation. In Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security. ACM, 29–36.

[82] Anna Sperotto, Ramin Sadre, Frank Van Vliet, and Aiko Pras. 2009. A labeled data set for flow-based intrusion detection. In International Workshop on IP Operations and Management. Springer, 39–50.

[83] Worachai Srimuang and Silada Intarasothonchun. 2015. Classification model of network intrusion using Weighted Extreme Learning Machine. In Computer science and software engineering (JCSSE), 2015 12th international joint conference on. IEEE, 190–194.

[84] Ming-Yang Su. 2011. Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest-neighbor classifiers. (2011), 3492-3498 pages. https://doi.org///doi.org/10.1016/j.eswa.2010.08.137 ID: 271506.

[85] Basant Subba, Santosh Biswas, and Sushanta Karmakar. 2016. Enhancing performance of anomaly based intrusion detection systems through dimensionality reduction using principal component analysis. In Advanced Networks and Telecommunications Systems (ANTS), 2016 IEEE International Conference on. IEEE, 1–6.

[86] Arief Rama Syarif and Windu Gata. 2017. Intrusion detection system using hybrid binary PSO and K-nearest neighborhood algorithm. In Information and Communication Technology and System (ICTS), 2017 11th International Conference on. IEEE, 181–186.

[87] Arman Tajbakhsh, Mohammad Rahmati, and Abdolreza Mirzaei. 2009. Intrusion detection using fuzzy association rules. (2009), 462-469 pages. https://doi.org///doi.org/10.1016/j.asoc.2008.06.001 ID: 272229.

[88] Xiaojun Tong, Zhu Wang, and Haining Yu. 2009. A research using hybrid RBF/Elman neural networks for intrusion detection system secure model. (2009), 1795-1801 pages. https://doi.org///doi.org/10.1016/j.cpc.2009.05.004 ID: 271575.

[89] Chau Tran, Tran Nguyen Vo, and Tran Ngoc Thinh. 2017. HA-IDS: A heterogeneous anomaly-based intrusion detection system. In Information and Computer Science, 2017 4th NAFOSTED Conference on. IEEE, 156–161.

[90] Tich Phuoc Tran, Longbing Cao, Dat Tran, and Cuong Duc Nguyen. 2009. Novel intrusion detection using probabilistic neural network and adaptive boosting. arXiv preprint arXiv:0911.0485 6, 1 (2009), 83–91.

[91] P Ravi Kiran Varma, V Valli Kumari, and S Srinivas Kumar. 2018. A Survey of Feature Selection Techniques in Intrusion Detection System: A Soft Computing Perspective. In Progress in Computing, Analytics and Networking. Springer, 785–793.

[92] Eduardo K. Viegas, Altair O. Santin, and Luiz S. Oliveira. 2017. Toward a reliable anomaly-based intrusion detection in real-world environments. Computer Networks 127 (2017), 200–216. https://doi.org///doi.org/10.1016/j.comnet.

2017.08.013 ID: 271990.

[93] Cynthia Wagner, Jérôme François, and Thomas Engel. 2011. Machine learning approach for ip-flow record anomaly detection. In International Conference on Research in Networking. Springer, 28–39.

[94] Gang Wang, Jinxing Hao, Jian Ma, and Lihua Huang. 2010. A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. (2010), 6225-6232 pages. https://doi.org///doi.org/10.1016/j.eswa.2010.02.102 ID: 271506.

[95] Shun-Sheng Wang, Kuo-Qin Yan, Shu-Ching Wang, and Chia-Wei Liu. 2011. An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks. (2011), 15234-15243 pages. https://doi.org///doi.org/10.1016/j.eswa.2011.05.076 ID: 271506.

[96] Donald Welch and Scott Lathrop. 2003. Wireless security threat taxonomy. In Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society. IEEE, 76–83.

[97] U. N. Wisesty and Adiwijaya. 2017. Comparative study of conjugate gradient to optimize learning process of neural network for Intrusion Detection System (IDS). In Science in Information Technology (ICSITech), 2017 3rd International Conference on. IEEE, 459–464.

[98] Su-Yun Wu and Ester Yen. 2009. Data mining-based intrusion detectors. (2009), 5605-5612 pages. https://doi.org///doi.org/10.1016/j.eswa.2008.06.138 ID: 271506.

[99] Cheng Xiang, Png Chin Yong, and Lim Swee Meng. 2008. Design of multiple-level hybrid classifier for intrusion detection system using Bayesian clustering and decision trees. (2008), 918-924 pages. https://doi.org///doi.org/10.1016/j.patrec.2008.01.008 ID: 271524.

[100] Binhan Xu, Shuyu Chen, Hancui Zhang, and Tianshu Wu. 2017. Incremental k-NN SVM method in intrusion detection. In Software Engineering and Service Science (ICSESS), 2017 8th IEEE International Conference on. IEEE, 712–717.

[101] Warusia Yassin, Nur Izura Udzir, Zaiton Muda, and Md Nasir Sulaiman. 2013. Anomaly-based intrusion detection through k-means clustering and naives bayes classification. In Proc. 4th Int. Conf. Comput. Informatics, ICOCI. 298–303.

[102] Yang Yi, Jiansheng Wu, and Wei Xu. 2011. Incremental SVM based on reserved set for network intrusion detection. (2011), 7698-7707 pages. https://doi.org///doi.org/10.1016/j.eswa.2010.12.141 ID: 271506.

[103] Chuanlong Yin, Yuefei Zhu, Jinlong Fei, and Xinzheng He. 2017. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access 5 (2017), 21954–21961.

[104] Dahlia Asyiqin Ahmad Zainaddin and Zurina Mohd Hanapi. 2013. Hybrid of fuzzy clustering neural network over NSL dataset for intrusion detection system. Journal of Computer Science 9, 3 (2013), 391–403.

[105] Shengchu Zhao, Wei Li, Tanveer Zia, and Albert Y. Zomaya. 2017. A Dimension Reduction Model and Classifier for Anomaly-Based Intrusion Detection in Internet of Things. In Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2017 IEEE 15th Intl. IEEE, 836–843.

[106] Chunjie Zhou, Shuang Huang, Naixue Xiong, Shuang-Hua Yang, Huiyun Li, Yuanqing Qin, and Xuan Li. 2015. Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation. IEEE Transactions on Systems, Man, and Cybernetics: Systems 45, 10 (2015), 1345–1360.